

ABSTRACT

A technique is disclosed for preventing un-authorized attachment of computer peripherals to a computer or computer network. Illustrative embodiments comprise two mating keyed-adapters between network/host computer ports and peripheral ports. One or both adapters can contain hardware for enabling and disabling communications to and from peripherals under software control from a host computer. The peripheral-side adapter contains a first hardware for storing a unique identifier corresponding to the attached peripheral. The host computer retrieves this stored identifier and compares it to a database of authorized identifiers. If a match is found, then communication to and from the peripheral is enabled either in a second hardware within the adapter or software within the host computer. If a match is not found, then communication to and from the peripheral is not permitted.